REDACTED

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT AND CRIMINAL COMPLAINT

I, Maria Leta-Leroux being first duly sworn state:

1. I am a citizen of the United States of America, and a resident of Virginia Beach, VA. I am 32 years old. I am a graduate of Excelsior College with a Bachelor of Arts and a graduate of Norwich University with a Master of Arts in Diplomacy. From March 2004 until July 2007, I was employed as a Police Officer with the City of Norfolk Police Department, Norfolk, VA, and served in various divisions, including: patrol, general crimes investigation squad, vice and narcotics, and gang squad, attaining the title of Detective. During that period, I received a significant number of hours in law enforcement training and investigations. From July 2007 through October 2008, I was employed by the Virginia Alcohol and Beverage Control Board (ABC) as a Special Agent assigned to investigate crimes related to violations of the Alcohol and Beverage Control laws of the Commonwealth of Virginia. During the course of my employment with the Virginia ABC, I conducted investigations in cases involving human trafficking, drug trafficking, gangs, prostitution, and counterfeit documents. From October 2008, until present, I have been employed by the Naval Criminal Investigative Service as a Special Agent assigned to the General Crimes Squad/Family - Sexual Violence Squad where I investigate crimes involving the receipt, transmission, and production of child pornography, and unlawful sexual acts with adults. During the course of my career in law enforcement, I have received training in investigations and have worked numerous cases including homicides, armed robberies, breaking and entering, forgery, and various fraud type cases. I have received computer training in Basic Data Recovery and Acquisition, computer previews using Access Data Forensic Tool Kit, computer peer-to-peer investigations, undercover on-line operations, computer investigative utilities, and various other subjects through the National Internet Crimes Against Children (ICAC) Task Force, and other training organizations. I am currently a member of the Southern Virginia Internet Crimes Against Children Task Force. I have previously written affidavits for search warrants in cases involving child pornography, gangs and other crimes.

2. This affidavit is made in support of an application for:

a. a warrant e of Scottie Lee NEZ, , Dumfries, VA , the ther described in hment A, to search for and seize instrumentalities, fruits, and evidence of violations of federal law, including: (a) Title 18 of the United States Code, Section 2251, which, in pertinent part, makes it a crime to produce child pornography; (b) Title 18 of the United States Code, Section 2252, which, in pertinent part, makes it a crime to knowingly mail, transport , ship, receive, or possess images of minors engaged in sexually explicit conduct, and (c) Title 18 of the United States Code, Section 2252A, which, in pertinent part, makes it a crime to knowingly mail, transport, ship, receive, or possess child pornography, as more particularly described in Attachment B.; and

b. a criminal complaint charging that Scottie Lee MARTINEZ, in and between July 2006 and December 2009, in the Eastern District of Virginia, and elsewhere, did and attempted to employ, use, persuade, induce, entice, and coerce a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct, and such visual depiction was produced using materials that had been mailed, shipped, and transported in interstate and foreign commerce by any means, including by computer, and such visual depiction had actually been transported in interstate and foreign commerce, in violation of Title 18, United States Code, Sections 2251(a) and (e)(2).

3. This affidavit will show:

a. there is probable cause that records and other items related to the violations being investigated (as specifically described in Attachment B, attached hereto and incorporated

herein) will be found at the SUBJECT PREMISES; and

b. that probable cause exists to believe that in and between July 2006 and December 2009, Scottie Lee MARTINEZ violated and attempted to violate 18 U.S.C. § 2251(a) which prohibits a person from employing, using, persuading, inducing, enticing, or coercing any minor to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct.

4. Because this affidavit is being submitted for the limited purpose of establishing probable cause for a warrant to search and for a criminal complaint, I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause. The information contained in this affidavit is based upon information provided by other law enforcement officers, my review of various documents and records, and, where specified, my personal observation and knowledge.

LEGAL AUTHORITY

5. 18 U.S.C. § 2251(a) provides that any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.

6. 18 U.S.C. § 2252(a) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, or possessing any visual depiction of minors engaging in sexually explicit conduct when such visual depiction was either mailed or shipped or transported in interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer or mails, or which contains materials which have been mailed or so shipped or transported, by any means including by computer. 18 U.S.C. § 2252A(a)(1) provides that any person who knowingly mails, or transports or ships using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography shall be punished.

7. 18 U.S.C. § 2252(a)(2) provides that any person who knowingly receives, or distributes, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, if (A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (B) such visual depiction is of such conduct, shall be punished. 18 U.S.C. § 2252A(a)(2)(A) makes it a federal criminal offense to knowingly receive or distribute any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

8. 18 U.S.C. § 2252(a)(4) provides that any person who (A) in the special maritime and territorial jurisdiction of the United States, or on any land or building owned by, leased to, or otherwise used by or under the control of the Government of the United States, or in the Indian country as defined in section 1151 of this title, knowingly possesses, or knowingly accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction; or (B) knowingly possesses, or knowingly accesses with intent to

view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if (i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (ii) such visual depiction is of such conduct shall be punished. 18 U.S.C. § 2252A(5)(B) makes it a federal criminaloffense for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

APPLICABLE DEFINITIONS

9. "Computer", as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

10. "Computer hardware", as used herein, consists of all equipment, which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such a fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to keyboards, printer, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms , or parts that can be used to restrict access

to computer hardware (including, but not limited to, physical keys and locks).

11. "Computer software", as used herein, is digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

12. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

13. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

14. "Child Pornography," as used herein, is defined pursuant to Title 18, United States Code, Section 2256(8), as "…any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where - (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct."

15. The term "minor," as used herein, is defined pursuant to Title 18, United States Code, Section 2256(1), as "any person under the age of eighteen years."

16. The term "sexually explicit conduct," as used herein, is defined pursuant to Title 18, United States Code, Section 2256(2) as "actual or simulated (A) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (B) bestiality; (C) masturbation; (D) sadistic or masochistic abuse; or (E) lascivious exhibition of the genitals or pubic area of any person."

COMPUTERS AND CHILD PORNOGRAPHY

17. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed and utilized. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computers and the Internet, distributors of child pornography use membership-based/subscription-based web sites to conduct business, allowing them to remain relatively anonymous.

18. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

19. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to

another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Insta-Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

20. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

21. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

22. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

23. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files.

Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software, when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS OF PRODUCERS AND COLLECTORS OF CHILD PORNOGRAPHY

24. Based on my training and experience, and the experiences of other law enforcement officers, which I am familiar with through training or similar joint investigations, I know the following behavioral characteristics to be consistent with subjects of this type of investigation:

25. Producers and collectors of child pornography almost always possess and maintain their "hard copies" and "digital copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Child pornography producers and collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, and videotapes for many years. Similarly, collectors of child pornography often maintain the collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection. The majority of individuals who collect and produce child pornography rarely, if ever, dispose of their sexually explicit materials. They often go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. Collectors and producers buying a new computer will usually transfer

their collection to the new computer or will save it to removable media before disposing of their old computer.

26. My training and experience have shown that users of the Internet who collect child pornography are very active collectors and often possess very large collections of child pornography. The widespread availability of the material, and the fact that nothing is required in return for the download, contribute to the ease of creating a large collection.

27. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEM

28. Your Affiant, based on conversations with trained Computer Investigative Specialists, who have been trained in the seizure, examination and retrieval of data from personal computer systems and related media, knows that searching and seizing information from computer systems often requires agents to seize all electronic storage devices to be searched later in a laboratory or other controlled environment.

29. Computer hardware, computer software, computer-related documentation, passwords, and data security devices may be important to a criminal investigation in three (3) important respects: (1) as instrumentalities for the violations of federal laws enumerated herein; (2) as devices used in conjunction with the collection and storage of electronic data and records related to the alleged violations, and (3) as fruits of illegal activity. Search and seizure of computer hardware, software, documentation, passwords, and data security devices, either as instrumentalities of criminal activity or as storage devices for evidence thereof, is contemplated at the Subject Premises.

30. Computer storage devices (like hard drives, diskettes, tapes, laser disks, and thumb or flash drives) can store enormous quantities of information. For instance, a single 2-gigabyte hard-drive is the electronic equivalent of approximately 1,000,000 pages of double-spaced text. However, unlike the search of documentary files, computers store data in files that are often not easily reviewed. Additionally, a suspect may try to conceal criminal evidence by storing files in random order and/or with deceptive file names. This may require the examiner to examine all the stored data to determine which particular files are evidence or instrumentalities of the crime. This sorting process can take weeks or months, depending on the volume of data stored.

31. Searching computer systems for criminal evidence is a highly technical process, requiring specialized skills and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which computer investigative specialist is qualified to analyze the system and its data. In any event, the investigative specialist will use certified forensic tools and data search protocols that are designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive code imbedded in the system as a booby trap), a controlled environment is essential to its complete and accurate analysis.

32. An important step that is ordinarily part of a forensic examination of a computer involves attempting to create an electronic "image" of those parts of the computer that are likely to store the evidence, fruits, instrumentalities, or contraband relating to the applicable offense. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files.

33. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the

Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

THE INVESTIGATION

34. On 01MAR10, Capt Janet Eberle, Staff Judge Advocate, USAF Joint Psychological Operations Task force (JPOTF), Camp As Sayliyah, Qatar, notified the Provost Marshal Office (PMO), Camp As Sayliyah, Qatar, that she identified suspected child pornography while logged onto the office network. Eberle stated while utilizing the office "white line," a morale line used in the office that allowed deployed users to surf the Internet, she opened the Home Sharing feature in the iTunes software application on her personal computer and saw a file named "(pthc) R@ygold****11yo" in the shared electronic library titled "Scottie's Frostwire Tunes." Eberle recognized the title as suspected child pornography from her experience as trial counsel at her home installation of Minot AFB. Eberle described "pthc" as the acronym for pre-teen hard core and "R@ygold" as the name of a child pornography series. Eberle stated the "****" stood for a portion of the filename she could not remember. Eberle contacted Chief

Petty Officer (CPO) Darryl Green, United States Navy (USN) and Captain Keith Moreno, United States Air Force (USAF), to attempt to identify the individual connected to the white line with the Home Share application open.

35. Moreno walked through the office spaces to find who was connected to the white line. Moreno knocked on Scottie Lee MARTINEZ's office door and MARTINEZ told Moreno to come in. Moreno saw, on MARTINEZ's personal laptop computer, that iTunes was running with Home Share activated. MARTINEZ had his I-Touch connected to the laptop. Moreno assisted MARTINEZ to attempt to transfer a photo from his laptop to the I-Touch then, when unsuccessful, MARTINEZ closed the laptop. Moreno reported to Eberle and she attempted to reconnect to "Scottie's Frostwire Tunes," however the connection was lost to that account.

36. Sean Banks, USAF Security Forces Investigator, PMO, Camp As Sayliyah, responded and obtained written consent from MARTINEZ for search and seizure of his personal laptop computer and Apple I-Touch on 01MAR10 and of his living quarters on 02MAR10. A search of the files on the laptop computer by J3-MEDEX Lab technicians resulted in a report of thousands of pornographic images and videos, several of which depicted suspected child pornography and files names which included terms indicative of child pornography to include, but not limited to: 10yo, preteen, kiddie, child, underage, incest, pedo, illegal, 15 years, young, angel, Lolita, step daughter, jailbait, youth, nymphets, 3yo, babyshivid, pedofilia, 8 yr old, reelkiddymov, pthc, 7yo, kinder, kids, 14y, grade 4, pupil, r@ygold, boyorgie, 11yo, and young boylovers.

37. MARTINEZ was an Inactive Navy Reservist who was activated in late June 2009, whereupon he traveled to Norfolk, VA circa 28JUN09 for pre-deployment work-up. MARTINEZ then traveled to South Carolina circa 03-04JUL09 for training prior to deploying to Qatar. Martinez returned to Norfolk from Qatar circa 12MAR10.

38. During an interview with law enforcement, MARTINEZ's current wife, Gindy Martinez, stated MARTINEZ obtained the personal laptop computer approximately two years ago while they lived in Dumfries, Virginia, the SUBJECT PREMISES, and brought the laptop with him when he deployed to Qatar. Gindy Martinez stated she also owned a laptop computer and the children shared a laptop computer in the playroom of

[redacted] at [redacted] T PR [redacted], Dumfries, VA [redacted],

39. The evidence seized by Banks pursuant to the consensual search and seizure was transferred to the Navy Criminal Investigative Service (NCIS), whereupon Rex Gray, NCIS Atlantic Cyber Division, initiated forensic examination of all electronic media. Preliminary results from the examination resulted in the identification of over 3000 images of child pornography, including images of prepubescent minors engaged in sexual acts with adults. Of those images, 44 known child pornography images preliminarily have been identified in the FBI Child Victims Identification Program (CVIP) index.. The files were created starting in March 2008 and continued until January 2010. During the majority of that time period, MARTINEZ lived in Dumfries, Virginia, the SUBJECT PREMISES.

40. In addition, approximately 600 images an[redacted] al[redacted] [redacted][2] [redacted] e[redacted] hed, nude, and engaged in sexual activity with MARTINEZ, to include, but not limited to, oral sex, vaginal penetration, kissing, fondling, and use of sex toys. One series of photographs depicts MARTINEZ in identical sexual acts with Jane Doe 1 that he had also photographed with his wife Gindy. The first images depicting Jane Doe 1 in sexually explicit conduct appear to have been made in July 2006 and the latest images appear to have been made circa 30DEC09.

[redacted] 27APR1[redacted] Doe 2, [redacted], DOB [redacted], and Ja[redacted] wed by [redacted] WEATHERFORD, Social Worker, Child Protective Services, Prince [redacted] unty, VA. Jane Doe 2 stated she has secrets wi[redacted] and that they play in her room, then stated [redacted] es not go into her room. Jane Doe 1 confirm[redacted] ous report that she showered with MARTINEZ, but stated she only reported it to get attention.

42. Jane Doe 2 and Jane Doe 1 were shown non-sexually explicit images extracted from MARTINEZ's computer that

---

[2] Pursuant to 18 U.S.C. § 3509(d), a generic term is used to protect the privacy of the minor victim and witnesses.

depicted the same backdrop as the pornographic images of Jane Doe 1. Jane Doe 2 and Jane Doe 1 i fied one image as being taken in MARTINEZ's bedroom in [redacted] Dumfries, VA house, the SUBJECT PREMISES, a room with t green painted walls and dark wooden furniture. Jane Doe 2 and Jane Doe 1 identified multi otographs as en in Jane Doe 1's bedroom in [redacted] Dumfries, VA [redacted], the SUBJECT PREMISES, a roo pink painted

43. On 19MAR10, Special Agent Bridgett Lucas interviewed MARTINEZ's ex-wife, Kerri Rotsch, who stated she saw suspected child porno [redacted] eturned alone to Texas to receive treatment for depression. Jane Doe 3 and Jane Doe 4 left Iceland in DEC04, and Jane Doe 4, who was then in 4th or 5th grade, reported to Rotsch that MARTINEZ "touched" her private area. ROTSCH stated she reported the allegation to the National Center for Missing and Exploited Children (NCMEC) and provided a hard drive with suspected images to law enforcement. The information was forwarded through the Houston, TX Innocent Images Task Force to NCIS via Defense Criminal Investigative Service (DCIS). The investigation was closed as unfounded for child pornography.

44. On 19MAR10, Special Agent Lucas interviewed Jane Doe 4 at her residence in Crestview, FL. Jane Doe 4 disclosed MARTINEZ began the sexual abuse when she was 6 years old when she lived in Oklahoma. Jane Doe 4 described anal penetration by MARTINEZ. Jane Doe 4 stated MARTINEZ designated her as his "favorite" and described on multiple occasions MARTINEZ took nude photographs of her. When in the bedroom with MARTINEZ, he would lay a towel on the bed to avoid soiling the sheets, and Jane Doe 4 would lie on her back on the towel. MARTINEZ would tie Jane Doe 4's hands with black ties and place lube from a blue jar on his penis then insert his penis into her anus. Jane Doe 4 stated MARTINEZ also had anal sex with her multiple times in the shower and would force Jane Doe 4 to perform oral sex on him, wherein he would ejaculate into her mouth. Jane Doe 4 stated MARTINEZ directed her not to tell anyone about the encounters. Jane Doe 4 also reported she saw suspected child pornography images on MARTINEZ's computer depicting a man with two girls.

45. Rotsch recalled more than one occasion when MARTINEZ was in Jane Doe 4's room with her bedroom door locked when Jane Doe 4 was in first or second grade. Jane Doe 3 s INEZ spent a lot of time alone with Jane Doe 4 in [redacted] in Iceland in the master bedroom with the door lo recalled an incident when Jane Doe 4 was crying because she did not want Jane Doe 3 to leave her alone in the house.

CONCLUSION

46. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause:

a. to believe that evidence that MARTINEZ employed, used, persuaded, induced, enticed or coerced the victim to engage in, or had a minor assist any other person in engaging in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, in violation of Title 18 U.S. Code, Section 2251(a) at [redacted] Dumfries, VA [redacted], the SUBJECT PREMISES; and that MARTINEZ did knowingly transport, mail, ship and receive in interstate or foreign commerce by any means, including by computer, child pornography in violation Title 18 U.S. Code, Sections 2252 and 2252A, at [redacted], Dumfries, VA [redacted], the SUBJECT PREMISES; and

b. to believe that in and between July 2006 and December 2009, in the Eastern District of Virginia, Scottie Lee MARTINEZ violated and attempted to violate 18 U.S.C. § 2251(a) which prohibits a person from employing, using, persuading, inducing, enticing, or coercing any minor to engage in sexually explicit conduct for the purpose of producing any visual depiction of such conduct.

47. Based upon my knowledge, training, and experience, and the experience and training of other law enforcement officers with whom I have had discussions, given the information provided above, it appears that there is a fair probability that contra ese crimes be located within [redacted], Dumfries, VA [redacted], the SUBJECT PREM

that within t sidence located at [redacted], Dumfries, VA [redacted], the SUBJECT specifically d bed in Attachment

B, attached hereto and incorporated herein, that constitutes evidence, fruits, and instrumentalities of the commission of said offenses.

49. Therefore, I request that:

a. a warrant be issued authorizing NCIS agents, with assistance from other law enforcement personnel, to search of said premises for the items noted in attachment B; and

b. a warrant be issued authorizing the arrest of Scottie Lee MARTINEZ.

_____
Maria Leta-Leroux
Special Agent
Naval Criminal Investigative Service

Subscribed and Sworn to before me this day _____ of _____, 2010.

_____
UNITED STATES MAGISTRATE JUDGE

Seen and Approved:

_____
Karen M. Somers
Special Assistant U.S. Attorney